保険・年金フォーカス

サイレントサイバーリスクの増大

サイバーリスクの引き受けは、サイバー保険にとどまらない!?

保険研究部 主席研究員　篠原　拓也
(03)3512-1823　tshino@nli-research.co.jp

1――はじめに

近年、急速に進むデジタル化に伴って、サイバーリスクが増大している。企業や個人を問わず、誰もが、パソコンやスマートフォンなどを通じたサイバー攻撃に、日常的にさらされている。

こうしたなか、損害保険会社は、サイバー保険の開発や引き受けを通じて、サイバーリスクへの補償を行っている。米国では、サイバーリスクの拡大とともに、保険会社が負うリスクも増大している。米国アクチュアリー・アカデミー(AAA)[1]は、「サイバーリスク　ツールキット」と題するペーパー(以下、「ペーパー」)を公表し、保険会社のリスク対応力の向上を促している。以下、そのペーパーをもとに、サイバーリスクについて見ていくこととしたい。(本稿は、特に断らない限り米国について記載。)

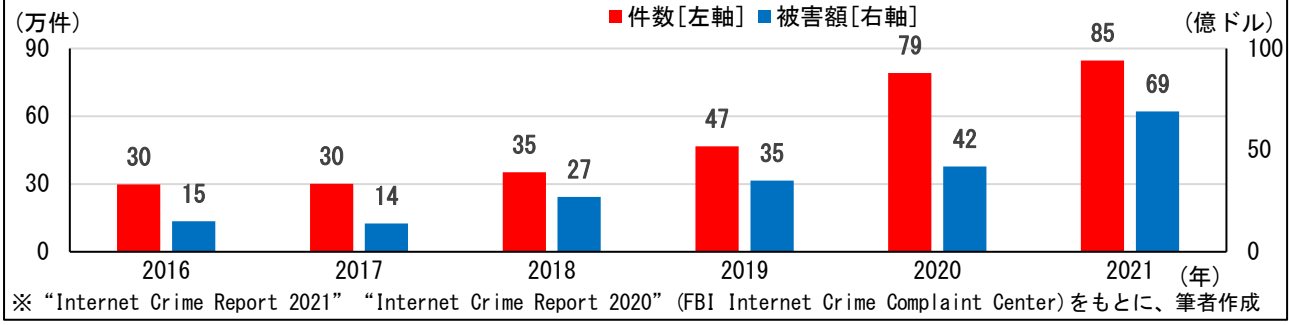
2――サイバーリスクの状況

まず、サイバー犯罪の推移やサイバー保険の普及の様子からみていこう。

1｜サイバー犯罪は顕著に増加している

サイバー犯罪の統計は、警察当局により定期的に公表されている。注意すべきなのは、こうした統計は発覚した犯罪分しかとらえていないことだ。仮に、ある企業のシステムにコンピューターウイルスが侵入して、データの書き換えや外部への流出などを行ったとしても、そのことが発覚しなければ、統計の数字には表れない。この統計は、少なくともこれだけあったという最低数を示すものといえる。

図表1. 米国のサイバー事件



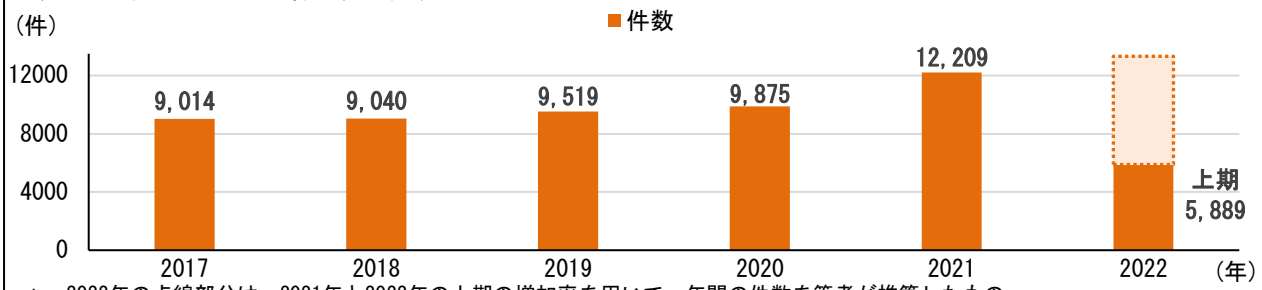
※“Internet Crime Report 2021” “Internet Crime Report 2020”(FBI Internet Crime Complaint Center)をもとに、筆者作成

[1] AAAは、American Academy of Actuariesの略。1965年に設立され、本部はワシントンD.C.。

図表１は、米国の状況だ。米国の政府機関である FBI のインターネット犯罪苦情センターが公表しているインターネット犯罪の苦情受付の推移を示している。ここ数年、件数、被害額とも増加しており、2021 年には被害額が大きく伸びたことがわかる。

図表２は、日本の状況で、警察庁が公表している検挙件数の推移を示している。日本でも、2021 年以降、件数が急増していることがうかがえる[2]。

図表2. 日本のサイバー犯罪の検挙件数

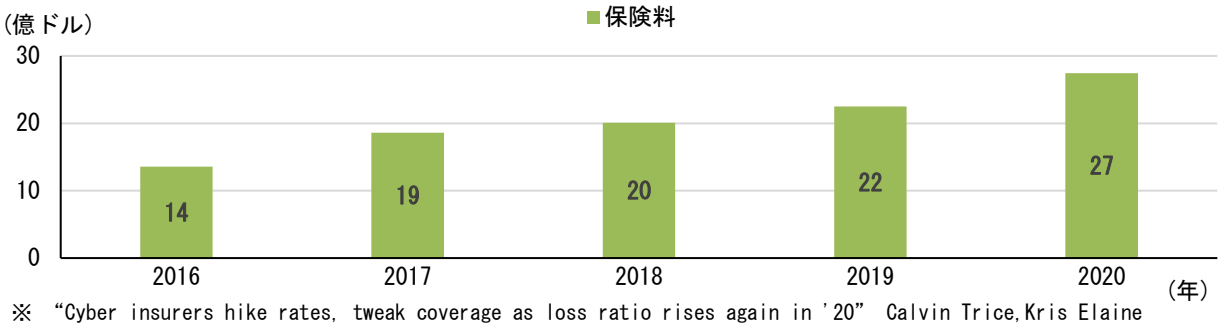


＊ 2022年の点線部分は、2021年と2022年の上期の増加率を用いて、年間の件数を筆者が推算したもの。
※「令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について」（警察庁，2022年9月15日）をもとに、筆者作成

2｜サイバー保険は普及途上

サイバー犯罪の増加に伴って、サイバー保険の普及が徐々に進んできた。図表３に見られるようにサイバー保険の保険料は、年々増加している。

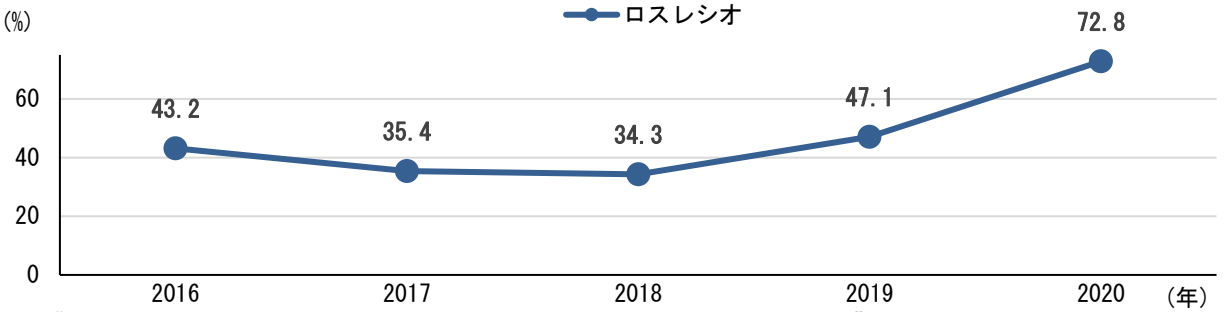
図表3. 米国のサイバー保険の普及



※ “Cyber insurers hike rates, tweak coverage as loss ratio rises again in '20” Calvin Trice, Kris Elaine Figuracion(S&P)とペーパーをもとに、筆者作成

一方、保険会社のロスレシオ(収入保険料に対して支払った保険金の割合)は、2020 年に急激に悪化している。サイバー犯罪の増加に伴って、保険給付が膨らんでいる様子がうかがえる。

図表4. 米国のサイバー保険のロスレシオ



※ “Cyber insurers hike rates, tweak coverage as loss ratio rises again in '20” Calvin Trice, Kris Elaine Figuracion(S&P)をもとに、筆者作成

[2] 総務省は情報通信白書のなかで、「様々な主体によりサイバーセキュリティに関する問題が引き起こす経済的損失が算出されているが、全世界で 6,000 億ドルから多いもので 22 兆 5,000 ドル、日本国内でも 1 社当たり数億円の損失が生じるものと算出されている」としている。（「令和 2 年版情報通信白書」（総務省）より）

今後、サイバーリスクの増大により、サイバー保険の注目度もさらに高まるものと考えられる。

3――サイバーリスクとは

ここで、サイバーリスクの種類や特徴について、おさえておこう。また、近年発生したサイバー犯罪をもとに、サイバーリスクの変質についてもみておこう。

1｜サイバー犯罪は顕著に増加している

サイバーリスクは、サイバー犯罪によってさまざまな被害が引き起こされるリスクといえる。サイバーリスクには、いくつかの分類方法がある。全米保険監督官協会(NAIC)によると、(1)個人情報の盗難、(2)業務の中断、(3)風評被害、(4)データ修復費用、(5)顧客リストや企業秘密の盗難、(6)ハードウェアやソフトウェアの修理費用、(7)影響を受けた消費者に対する信用モニタリングサービス、(8)訴訟費用、といったリスクが含まれるという[3]。

2｜サイバー攻撃にはさまざまな種類がある

ひと口にサイバー攻撃といっても、ランサムウェアのように特定のターゲットを狙う攻撃もあれば、フィッシング詐欺のような不特定多数の人を狙う攻撃もある。次の表では、主なサイバー攻撃をまとめた。サイバー攻撃にはさまざまな種類があることがみてとれる。

図表 5. 主なサイバー攻撃

	概要
不正アクセス	利用する権限を与えられていないコンピュータに対して、不正に接続しようとすること。実際にそのコンピュータに侵入したり、利用したりすることを不正アクセスに含むこともある。
標的型攻撃	特定の組織を狙って、機密情報や知的財産、アカウント情報(ID、パスワード)などを窃取しようとする攻撃。この攻撃では、標的の組織がよくやり取りをする形式のメールを送りつけ、そこについている添付ファイルやリンクをクリックさせて、そこからマルウェア配布サイトに誘導するといった手口がよく使われる。敵対する特定の組織に長期間持続的に攻撃するものは、「高度標的型攻撃」と呼ばれる。
バックドア	ウイルス感染により、コンピュータに、外部から侵入するためのバックドア(裏口)が作成される。この種のウイルスに感染したコンピュータは、外部から自由に操作される恐れがある。
パスワードクラッキング	パスワードの可能な組み合わせを全て試す「ブルートフォースアタック」、よく使われる単語を登録した辞書をもとに順番に試す「辞書攻撃」、一度漏洩したパスワードを使って他のサイトのログインをはかる「パスワードリスト攻撃」などにより、パスワードを突破する。
DDoS 攻撃[4] (ディー・ドス攻撃)	Web サーバやメールサーバなどに対して、複数のコンピュータから大量のサービス要求のパケットを送りつけることで、相手のサーバやネットワークに過大な負荷をかけ、使用不能にする。同様の攻撃方法である DoS 攻撃は、1 台のコンピュータから実行するもの。DDoS 攻撃の場合は、第三者のコンピュータを感染させておくなどして、攻撃者の指示によって、複数のコンピュータが一斉に攻撃を行う。
フィッシング詐欺	実在の金融機関(銀行やクレジットカード会社)、ショッピングサイトなどを装ったメールを送付し、これらのホームページとそっくりの偽のサイトに誘導して、住所、氏名、銀行口座番号、クレジットカード番号などの重要な情報を入力させて詐取する行為のこと。
なりすまし	他の利用者のふりをすること。または、中間者(Man-in-the-Middle)攻撃など、他の利用者のふりをして行う不正行為のこと。例えば、その当人であるふりをして電子メールを送信したり、別人のふりをして電子掲示板に書き込みを行ったりする行為が挙げられる。
ランサムウェア	実在する知人などからの返信を装って情報窃取等を行う Emotet(エモテット)などの感染により、端末の一部機能を使用不能にしたり、ファイルを暗号化して使用できなくしたりする。そして、それらを使用可能とするための、身代金を要求する。

※「国民のための情報セキュリティサイト」(総務省, http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html)等を参考に、筆者作成

[3] “Cybersecurity” (NAIC, Last Updated 2021.5.27)より。
[4] DDoS は、Distributed Denial of Service の略。分散型サービス拒否攻撃を指す。

3｜個人向けはフィッシング、組織向けはランサムウェアが最大の脅威

それでは、実際に、どういった事象が脅威として挙げられているのか。情報処理推進機構セキュリティセンターが示している「情報セキュリティ 10 大脅威 2022」[5]によると、個人向けは、フィッシングによる個人情報等の詐取。組織向けは、ランサムウェアによる被害が最大の脅威とされている。ランサムウェアによる被害は、組織向けでは、昨年に続いて最大の脅威と位置づけられている。

図表 6. 情報セキュリティ上の 10 大脅威

順位	個人向け	組織向け
1	フィッシングによる個人情報等の詐取	ランサムウェアによる被害
2	ネット上の誹謗・中傷・デマ	標的型攻撃による機密情報の窃取
3	メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	サプライチェーンの弱点を悪用した攻撃
4	クレジットカード情報の不正利用	テレワーク等のニューノーマルな働き方を狙った攻撃
5	スマホ決済の不正利用	内部不正による情報漏えい
6	偽警告によるインターネット詐欺	脆弱性対策情報の公開に伴う悪用増加
7	不正アプリによるスマートフォン利用者への被害	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
8	インターネット上のサービスからの個人情報の窃取	ビジネスメール詐欺による金銭被害
9	インターネットバンキングの不正利用	予期せぬ IT 基盤の障害に伴う業務停止
10	インターネット上のサービスへの不正ログイン	不注意による情報漏えい等の被害

※ 「情報セキュリティ 10 大脅威 2022」（独立行政法人 情報処理推進機構セキュリティセンター，2022 年 3 月）をもとに、筆者作成

4――サイバーリスクの特徴

サイバーリスクを他のリスクと比較してみたときに、どういう特徴が挙げられるのか。

1｜サイバーリスクには集積性の際限がない

サイバーリスクは、リスクの発現が同時期に集中する「集積性」をもつ。たとえば、フィッシング詐欺では、ある時期に不特定多数の人に一斉にメールを送付して、詐欺被害が多発する。こうした集積性は、地震や台風のような大規模自然災害でもみられる。だが、サイバーリスクの場合は地震の活断層や台風の襲来する季節のような、地理や時間による制限がない。このため、いつでもどこでも起こりうるという特徴を持つ。極端な場合、全世界で同時期にリスクが多発することもありうる。

2｜サイバーリスクは人為的に起きる

当たり前のことだが、サイバーリスクは人間の手によって起こされる。情報取扱者の不注意や過失によって漏洩などの問題が起きることもあるが、サイバー攻撃の場合は、攻撃者が意図的に引き起こす。攻撃者は、セキュリティの整備状況に応じて、動的に攻撃を変えることができる。そのため、サイバーリスクは発現にランダム性がないとされている。たとえば、あるシステムに、脆弱性の放置など、サイバーセキュリティ上の欠陥があると、その欠陥をつくマルウェア[6]がつぎつぎにあらわれる恐れがある。

---

[5] 情報セキュリティ専門家を中心に構成する「10 大脅威選考会」の協力により、2021 年に発生したセキュリティ事故や攻撃の状況等から脅威を選出し、投票により順位付けして解説した資料。

[6] 悪意のあるソフトウェアや悪質なコードの総称。

3｜サイバーリスクはICTの進化とともに脅威が増す

サイバーリスクはネット環境の発展とともに、攻撃などの機会が増える。近年、モノのインターネット(Internet of Things, IoT)の拡大により、スマートスピーカー等のデジタル情報家電など、ネット経由で制御可能なデバイス数が増加している。これにより、サイバーリスクの脅威が増している。

2020年以降、コロナ禍によりリモートワークが進んだことで、コンピューターウイルスが従業員の自宅パソコン等を通じて企業のシステムに侵入する可能性が出てきている。コロナ禍は、感染症のウイルスとコンピューターウイルスの2つのウイルスにより、リスクを増大させたといえる。

4｜サイバーリスクは、リスク管理上、過去の経験を生かしにくい

上記の3つの特徴は、サイバーリスクの管理の難しさにつながる。リスク管理上、リスクの集積に際限がなく、リスク発現にランダム性がないとされており、しかもその脅威は今後ますます増加していく。このため、過去に発生したサイバーリスク事象の経験を生かすだけでは、将来のリスク管理は不十分となる。

このことは、サイバー保険の開発や引き受けにおいて、特有の検討要素につながっていく。つまり、サイバーリスクの価格や引受条件は、単に過去の経験データをもとに設定するだけでは不十分となる。今後のリスクの増大や変質の見通しを立てながら、検討していく必要がある。

5――サイレントサイバーリスク

保険会社は、サイバーリスクをサイバー保険として取り扱うだけではない。一般の損害保険にも、サイバーリスクの影響が出る可能性がある。こうした一般の保険での給付への影響は、保険会社にとって「サイレントサイバーリスク」といわれる。本章では、このリスクについて、みていこう。

1｜サイレントサイバーリスクは、契約規定のあいまいさに起因する

一般の保険契約では、契約規定のなかにサイバーリスクが明示的に含まれていない場合や、明確に免責とされていない場合がある。こうした場合、サイバー事件による損害保険の補償(損害賠償補償など)の範囲があいまいになる。保険会社側からみると、補償を提供する意図がなかった保険契約からも、サイバー攻撃によって、保険金請求が発生する事態が生じることとなる。

たとえば、洪水保険のような自然災害を対象とした補償を行う保険にも、サイバーリスクは存在する。サイバー攻撃によって、ダムの制御システムがハッキングされて洪水が発生し、その結果、甚大な被害が生じたとしよう。この場合、保険契約上、サイバー攻撃による洪水に関する給付支払の規定があいまいだと、保険会社は、保険金支払いによる損失のリスクにさらされる可能性がある。

2｜サイレントサイバーリスクは、意図せざる補償と価格未設定の補償からなる

サイレントサイバーリスクは契約規定上、保険会社が意図していなかった補償から発生するが、それればかりではない。たとえ契約規定に補償の内容が明文化されていたとしても、その保険料設定の見積もりが不適切な場合、想定を上回る保険金支払いが起こり、損失発生につながる恐れがある。

先ほどの洪水保険の例で、サイバー攻撃により発生する洪水を補償すると規定して、それに応じた保険料を設定していた場合を考えてみよう。価格設定に用いた前提(過去の経験データ等による)を、サイバーリスクの増大に伴って改定しておかないと、保険金が想定を超えてしまうことがある。サイ

バーリスクが年々増大すれば、それを補償する保険契約の保険料も毎年上昇していくことにつながる。

3｜ウクライナに向けたサイバー攻撃が、サイレントサイバーリスクへの注目を集めるきっかけとなった

サイレントサイバーリスクが、広く知られるきっかけになったサイバー攻撃がある。

2017 年 6 月に発生したマルウェア “NotPetya”（ノットペーチャ）[7]によるサイバー攻撃だ。このサイバー攻撃は、主にウクライナに焦点を当てており、ロシアによるものとされた[8]。海運業や運送業の大手など、複数のグローバル企業にも事業の中断などの形で、被害をもたらした。被害総額は 100 億ドル超と推定されている。これに伴い、これらの企業が契約していた保険では、一般賠償責任などの形でサイバー損失が発生した。

このサイバー攻撃の後、損害保険契約で「戦争行為免責」を理由に、保険金の支払いを拒否する事案が発生した。この契約の保険金支払いを巡って、契約者企業と保険会社の間で訴訟[9]が発生しており、それをきっかけにサイレントサイバーリスクへの注目度も高まった。

保険会社では、サイバーリスクに関する契約規定を明確化する動きが出ている。

6――おわりに（私見）

以上、近年高まりつつあるサイバーリスクについて、概観していった。このリスクは、今後もさらに増大することが考えられる。

サイバーリスクは、社会のデジタル化に伴い、主要なリスクの 1 つとなっていくだろう。短時間のうち被害が国境を超えて拡大する恐れがある、脆弱性を狙って攻撃が繰り返されるなど、他のリスクにはみられない脅威となることも考えられる。

保険会社にとっては、サイレントサイバーリスクとして、サイバー保険以外の保険契約にも、影響が及ぶ可能性があるため、契約規定の確認を行うことが必要となるだろう。

今後も、サイバーリスクとそれに対する保険会社の取り組み動向について、注視していきたい。

---

[7] 2016 年 3 月にウクライナで発生した“Petya”というマルウェアに似ていたが、感染力が強く、「Petya ではない」と名付けられた。

[8] 2018 年に、米国、英国、オーストラリアの政府は公式に攻撃がロシア軍によるものだとしたが、その証拠は公表されていない。

[9] Mondelez International, Inc. v. Zurich American Insurance Company 2018 WL 4941760 (Il.Cir. Ct.) No.2018L022008 (NotPetya サイバー攻撃に関する損害保険訴訟)